

Агентный портал: пакет для службы ИБ

Модель угроз, меры защиты и условия допуска

Параметр	Значение
Версия / дата	0.1 / 02 октября 2026 года
Статус	Проект для обсуждения и последующего согласования
Объект	Портал, подключение моделей, агентные сценарии и эксплуатация
Граница	Развёртывание, обучение и GPU-инфраструктура моделей вне проекта
Документ	Материалы для review информационной безопасности

Принцип: пользователь собирает помощника из разрешённых возможностей; платформа обеспечивает доступ, бюджет, выполнение и проверяемый результат.

Сроки, ресурсы и целевые показатели являются проектными оценками. Функциональность не объявляется уже реализованной. Выбор агентного runtime подтверждается сравнительными испытаниями.

Содержание

1. Назначение пакета и статус согласования	3
2. Активы, классификация и ответственность	4
3. Границы доверия и потоки данных	5
4. Идентификация и привилегированные роли	7
5. Авторизация объектов и совместный доступ	8
6. Модельные подключения и внешняя передача	9
7. Сеть, egress, DNS и SSRF	10
8. Prompt injection, документы и веб-контент	11
9. Изоляция кода и execution-сред	12
10. MCP, плагины и SMTP	13
11. Секреты, криптография и журналирование	14
12. Supply chain, обновления и конфигурация	15
13. Backup, устойчивость и инциденты	16
14. Реестр угроз и остаточных рисков	17
15. Программа security-проверок	18
16. Перечень документов и форма допуска	20

1. Назначение пакета и статус согласования

Документ предназначен для архитектурного review и подготовки допуска корпоративного агентного портала к пилоту и эксплуатации. Он описывает предложенные меры, необходимые данные и доказательства проверки. Меры ещё не объявляются реализованными; фактические результаты заполняются на этапах разработки и приёмки.

Объект review — портал, каталог подключений моделей, runtime workers, инструменты, документы, аналитика, execution-среды и инфраструктура приложения. Модели рассматриваются как отдельно предоставляемые API. Их GPU, обучение и inference-инфраструктура не включены в проект. Обязательны контракт доступа и ответственность владельца API.

Организация должна предоставить применимые внутренние нормы, категории данных, правовую юрисдикцию и требования к контролям. Пакет не утверждает соответствие конкретному стандарту, сертификацию, выполнение обязательных норм или невозможность утечек.

Контрольная точка	Что согласуется	Статус проекта
Security design review	Границы, данные, идентичности и egress	Требует review
Допуск пилота	Ограниченная аудитория, данные, endpoints и ограничения	Требует review
Допуск production	Evidence тестов, residual risks, эксплуатация и владельцы	Требует review
Изменение внешних интеграций	Новый endpoint, класс данных или привилегия	По change process

В пакет входят описание trust zones, матрица доступа, контрольная модель, реестр угроз, набор испытаний, эксплуатационные регламенты и форма подписания. Локальный HTML-макет использует синтетические данные и не подтверждает безопасность production.

2. Активы, классификация и ответственность

Актив	Ценность / чувствительность	Ответственный
Документы и базы знаний	Корпоративная информация и возможные персональные данные	Владелец данных / пространства
Prompt, ответы и артефакты	Производные данные исходных документов	Владелец задания и политики данных
Пользователи, группы, роли	Полномочия доступа	IAM + администратор платформы
Ключи модельных API/инструментов	Доступ к внешним и внутренним системам	Владельцы подключений / secret service
Ledger и бюджеты	Учёт расхода, финансирование и контроль	Владелец бюджетного счёта
Конфигурация помощника/сценария	Полномочия выполнения и бизнес-логика	Автор + владелец публикации
Runtime и песочницы	Выполнение недоверенного кода	Оператор execution-pool
Аналитика и sharing-события	Использование сотрудниками и структура доступа	Владелец аналитики + ИБ
Audit/backup/release bundle	Расследование, восстановление и цепочка поставки	Оператор + ИБ

Предлагаемые классы: публичные, внутренние, ограниченные. Организация может заменить их своей классификацией. Производные данные, summaries, embeddings и артефакты наследуют ограничения источника либо получают более строгую категорию. Модельный ответ не считается обезличенным автоматически.

Для каждого класса определяется: допустимые model endpoints; разрешение внешнего search; SMTP-адресаты; срок хранения; аудит; экспорт; резервные копии и условия удаления. Класс передаётся вместе с объектом через pipeline и сохраняется в metadata.

Перед production необходим реестр владельцев данных и правило определения категории при отсутствии метки. Предлагаемое безопасное правило — ограниченный доступ до классификации, а не свободная передача внешнему API.

3. Границы доверия и потоки данных

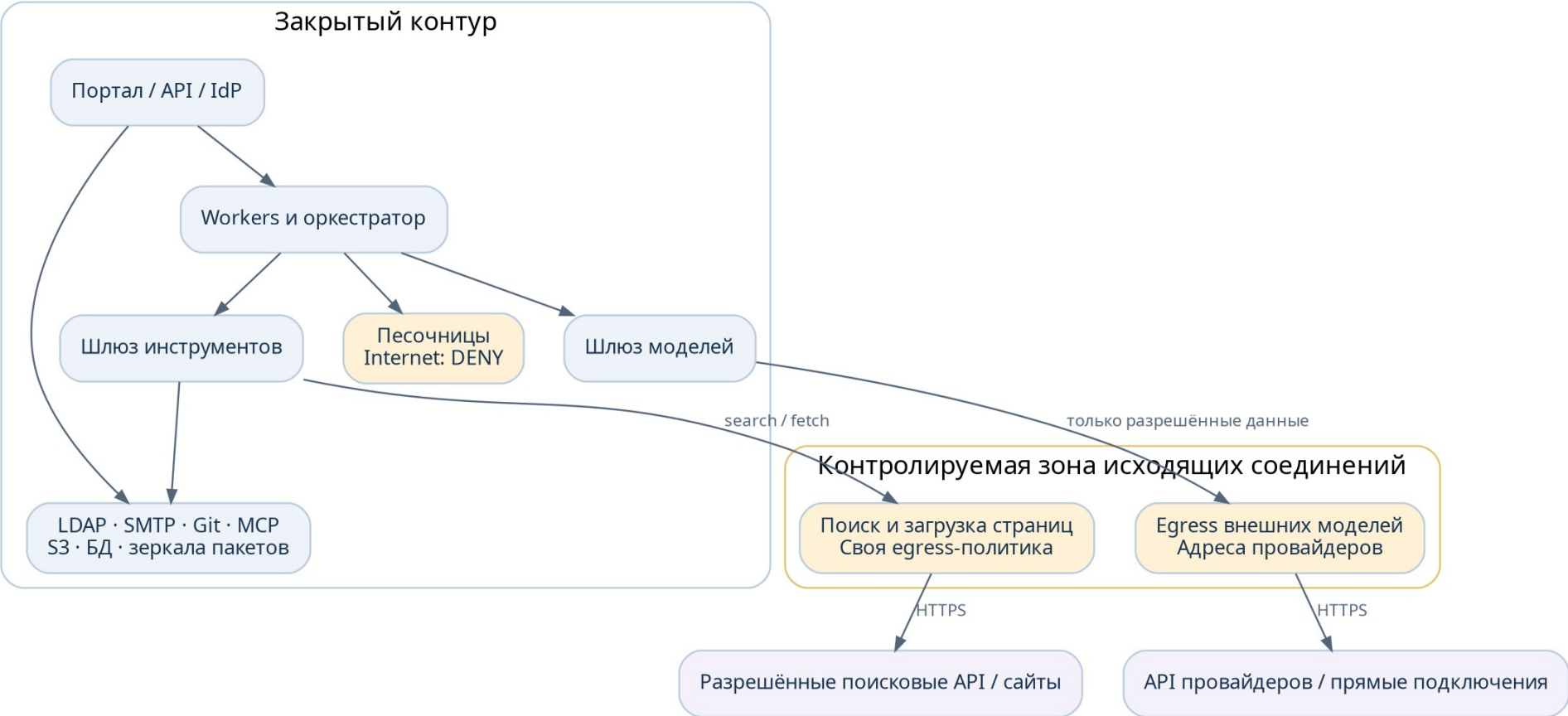


Рисунок 1. Контур приложения и выделенные исходящие направления.

Trust zones: пользовательские устройства; application/control plane; data services; runtime workers; изолированный execution-pool; search/fetch zone; model egress; корпоративные системы; административная зона; release-import/backup. Размещение zone может быть логическим или сетевым, но ограничения должны подтверждаться фактическим firewall/ACL.

Поток	Какие данные передаются	Проверка перед передачей
Браузер → API	Запрос, файлы и выбор помощника	Auth, CSRF/session protection, ACL, size/type
API → runtime	Run, версия помощника, ссылки на контекст	Идентичность run и policy revision
Runtime → model gateway	Разрешённый контекст и параметры	ACL, класс данных, budget и endpoint policy
Gateway → внешний API	Только данные разрешённой категории	Зарегистрированный маршрут, TLS и provider rules
Runtime → tool gateway	Инструмент и ограниченные аргументы	Server identity, разрешение и согласование
Search → интернет	Поисковый запрос / URL	Политика передачи данных и SSRF
Документ → parsing/RAG	Файл, текст, chunks и embeddings	Quarantine, execution limits и ACL
Tool → SMTP/Git/MCP	Проверенные параметры внешнего эффекта	Sender/repository/tool scope и idempotency policy
Services → telemetry	Минимальные события и метрики	Redaction и разрешённый внутренний destination

Search query — канал передачи информации наружу. Отсутствие интернета у shell не исключает утечку через разрешённый search или внешний API. Модель не уполномочена самостоятельно снять ограничение категории данных.

4. Идентификация и привилегированные роли

OIDC используется для portal sessions. LDAP/AD федерация либо корпоративный IdP — источник пользовательских идентичностей и групп. Локальные пользователи предусмотрены по утверждённой политике. Приложение не хранит LDAP-пароли в собственных таблицах.

Роль	Допустимая область	Ограничение
Пользователь	Свои runs и разрешённые пространства	Нет регистрации endpoints и изменения глобальных политик
Автор	Помощники/сценарии в своей области	Публикация не передаёт его личные права
Руководитель	Командные лимиты и доступ	Только делегированные бюджеты и объекты
Администратор	Конфигурация и подключения	Не автоматическое право читать документы
Оператор	Серверы, queues и deployment	Нет общего доступа к prompts/файлам
Аудитор	Разрешённые журналы	Содержание документов по отдельному ACL
Сервисный principal	Конкретный connector/schedule	Минимальный scope, срок и владелец

Привилегированные действия используют MFA через IdP и при необходимости review второй роли. Аварийные локальные аккаунты ограничены, проверяются и журналируются. Регламент восстановления доступа не предполагает общего опубликованного admin-password.

Отзыв роли и блокировка проверяются на сервере перед каждым новым действием и продолжением задания. Устаревшие JWT/groups caches не должны бессечно сохранять права. Согласовать и измерить максимальную задержку отзыва; предлагаемый ориентир — до пяти минут для обычной синхронизации и немедленный deny новых действий для административной блокировки.

5. Авторизация объектов и совместный доступ

Контроль доступа распространяется на UI, API, SSE, object download, retrieval, артефакты, snapshots, exports и аналитические агрегаты. Все ссылки на объекты повторно проверяются; знание object ID не считается правом доступа.

Эффективные права — пересечение principal, пространства, помощника и глобальной политики. Нельзя использовать привилегии автора опубликованного помощника для чтения его личных документов от имени другого сотрудника. Tools получают идентичность из server-established run context, а не из аргументов модели.

Sharing-операция	Обязательные условия
Grant документу	Владелец вправе делегировать указанную роль и аудиторию
Grant группе	Проверена реальная группа и актуальное membership
Публикация помощника	Инструкция/артефакты не содержат скрытого чужого контекста
Доступ tool	Разрешённый tool scope; downstream-авторизация проверена
Временное разрешение	Срок, причина и автоматический revoke
Export/share link	Ограниченный срок и scope; отсутствие публичного доступа по умолчанию

Доступ и фактическое использование — разные audit events. Dashboard не раскрывает закрытые названия документов, сотрудников или пространств через top lists. Кэши сегментируются по ACL-equivalent score; изменение доступа инвалидирует применимые записи.

Негативные тесты включают прямой запрос чужого object ID, подмену workspace, просроченный share link, role escalation, экспорт чужих данных и чтение старого кэша после revoke.

6. Модельные подключения и внешняя передача

Администратор регистрирует API модели, capabilities, secret_ref, доверенный CA, маршрут, разрешённые группы и классы данных. Проверяется реальный тип API, usage, output limit и ошибки. Model gateway — единственная точка передачи модельных запросов из runtime.

Для внешнего API нужно отдельное решение о допустимости данных: какой контент передаётся, какие договорные/организационные ограничения действуют и кто является владельцем подключения. Эти условия предоставляет организация; документ не предполагает одинаковые правила у всех провайдеров.

Контроль	Проектное требование
Endpoint allowlist	URL задаёт уполномоченная роль; произвольный user endpoint закрыт в R1
Секрет	Не передаётся harness, sandbox или браузеру
TLS	Проверка hostname/CA; отключение verify не штатный режим
Fallback	Только разрешённые подключения с сохранением класса данных
Payload	Отсутствие чужого контекста; нормализованные параметры
Usage	Подтверждённый факт или явная отметка unknown; ledger reservations
Telemetry	Полные prompts/ответы не экспортируются по умолчанию
Disable	Новые вызовы прекращаются; активные действия обрабатываются по регламенту

Cloud managed harness не считается размещённым в закрытом контуре только потому, что sandbox локальный. Необходимо отдельно определить, где находятся control plane, history и исполнение агентного цикла.

7. Сеть, egress, DNS и SSRF

В production разрешения устанавливаются по точным источникам, назначениям и протоколам. Список ниже дополняет основную матрицу документа архитектуры и превращается в утверждённые firewall rules.

Источник	Разрешённые назначения	Запрещено по умолчанию
Браузер	Portal/IdP 443	Прямые data/control endpoints
Runtime worker	Model/tool gateway, Temporal, назначенные data services	Общий интернет и произвольный проху
Песочница	Только назначенные internal mirrors и workspace API	Интернет, LDAP, SMTP, management API, cloud metadata
Model gateway	Зарегистрированные API через нужный egress	Неограниченное HTTP-fetch
Search/fetch	Согласованные engines/sites через отдельную политику	Internal admin, loopback, link-local и metadata
Deployment runner	Только inventory targets и registry	Произвольная сеть по входным параметрам пользователя
Telemetry	Внутренний collector/SIEM	Публичный tracing SaaS без отдельного разрешения

URL-проверка учитывает scheme, port, userinfo, DNS, IPv4/IPv6 и redirect chain. Запрет private IP применяется к фактическому соединению, чтобы не допустить DNS rebinding. Internal connectors отделяются от internet-fetch. Однократная проверка hostname перед подключением недостаточна.

Учитываются Docker forwarding/NAT, host networking, IPv6 и DNS leakage. Compose bridge сам по себе не гарантирует deny egress. Default-deny проверяется из worker и sandbox с packet/log evidence. Недопустим обход через curl, tool, MCP registration, package manager либо внешний браузер.

Admin-интерфейсы открываются только в административной зоне. Порты optional Nomad/Kubernetes не открываются, если этот профиль не используется.

8. Prompt injection, документы и веб-контент

Документы, результаты поиска, сообщения инструментов и содержимое репозитория являются недоверенными входными данными. Инструкция внутри них не изменяет system policy, identity, budget или permissions. Ограничения enforced сервером даже при ошибке модели.

Сценарий атаки	Мера	Проверяемое доказательство
Документ требует отправить секрет	Секреты недоступны модели; tool authorization	Тест с вредоносным документом
Сайт подменяет инструкцию пользователя	Отделение retrieved data и tool scopes	Payload/decision trace без лишнего содержимого
Результат tool содержит исполняемую команду	Команда допускается только разрешённым sandbox-профилем	Попытка выйти за permissions отклонена
Ответ заставляет открыть внутренний URL	SSRF controls и отдельные connectors	Private-IP/redirect tests
Подмена цитаты	Источник проверяется по сохранённой версии/ACL	Citation validation
Вредоносный файл/архив	MIME, quarantine, parser limits и запрет макросов	Malformed/oversized fixtures

Фильтрация prompt injection может использоваться как дополнительный слой, но не как единственное основание безопасности. Запрет утечки нельзя доказывать только тестом нескольких формулировок или заключением LLM-as-judge.

Parser/OCR запускается с deadline, памятью и ограниченной сетью. Архивы отключены в R1; при включении нужны пределы вложенности и распаковки. Пользователь видит отказ повреждённого файла; инфраструктурная трассировка не возвращается ему полностью.

9. Изоляция кода и execution-сред

Песочницы размещаются на выделенном execution-pool. Они не имеют ключей модельных API, LDAP, SMTP, platform management и общего host Docker socket. Executor создаёт среду через ограниченный управляющий API; непривилегированный пользовательский код не управляет этим API.

Минимальные меры: user namespace/rootless или эквивалент по выбранному runtime; dropped capabilities; seccomp/AppArmor/SELinux где применимо; read-only base image; выделенный workspace; CPU/RAM/PID/disk limits; network deny; ограничение mounts; TTL; проверенный teardown. Конкретный набор подтверждается выбранной ОС и runtime.

Для усиленной изоляции рассматривается gVisor или отдельная VM. Это не абсолютная гарантия от escape; поддержка необходимых компиляторов и браузерных тестов проверяется до включения профиля. Обычный shell в процессе shared web API не допускается.

Контрольная задача	Ожидаемый результат
Прочитать host secrets	Запрет; секреты отсутствуют в mounts/env
Подключиться к management socket/API	Запрет на network/filesystem уровне
Запустить fork bomb / заполнить диск	Локальное ограничение и остановка; другие runs доступны
Выполнить интернет-запрос	Запрет IPv4/IPv6/proxy путей
Доступить чужой workspace	Запрет идентичности, путей и object ACL
Продолжить после revoke/cancel	Новые шаги закрыты; resource cleanup подтверждён

Git push и изменения внешних систем — отдельные capabilities. Доступ к репозиторию выдаётся минимальный и scoped. Восстановление задания не повторяет без проверки уже выполненный внешний эффект.

10. MCP, плагины и SMTP

Реестр расширений содержит владельца, версию, источник, schemas, права, endpoints и семантику операций. Администратор подтверждает публикацию. Tools исполняются через gateway; generated user_id не заменяет авторизацию. MCP transport и authentication выбираются по конкретной версии протокола и системы.

Интеграция	Риски	Обязательные меры
MCP	SSRF, confused deputy, лишние права и небезопасные resources	Allowlist, server auth, per-tool ACL, validation и review
Плагин	Supply chain, произвольный код, утечка секретов	Отдельный service/container, digest, minimal secrets/network
SMTP	Утечка вложений, массовая рассылка, impersonation	Sender/recipient rules, attachment controls, quota и audit
Git	Утечка кода, destructive push и credentials	Repository scope, least privilege, review и secret isolation

Согласование привязано к точному действию, параметрам и сроку. После изменения адресатов или вложения решение становится недействительным. Approval UI показывает достаточно данных для осмысленного решения, но не чужую секретную информацию.

Почтовая outbox снижает риск дублей, но SMTP не обеспечивает exactly-once. Неоднозначный результат передаётся в регламент review; автоматический retry может привести к повторной отправке и должен быть ограничен.

Отключение плагина прекращает новые calls. Уже выполненные действия не считаются отменёнными. Manifest/export никогда не содержит credentials.

11. Секреты, криптография и журналирование

Секреты хранятся в корпоративном secret store либо защищённой сервисной конфигурации с разграничением файловых прав. Предпочтительно использовать уже существующий сервис. Новое хранилище секретов вводится только с готовой эксплуатацией, recovery и назначенным владельцем.

Ротация, отзыв и аварийная замена проверяются на тестовом окружении. Разные сервисы имеют разные учётные записи; общая master-key, доступная всем workers, не применяется. Отсутствие секретов в logs, errors, exported configurations, backups без защиты и browser storage проверяется.

TLS используется на межзоновых и чувствительных сервисных связях. Проверяются corporate CA, hostname, срок сертификата и доступный механизм обновления. Key handling и шифрование дисков/backups задаются корпоративной политикой; алгоритмы и соответствие конкретным нормам не утверждаются без требований организации.

Журнал	Хранить	Исключать / ограничивать
Auth	Principal, результат, источник и время	Пароли, refresh/access tokens
Config	Revision, actor, scope, status	Secret values
Run/model	IDs, connection, usage, duration и error category	Полный prompt/response по умолчанию
Tool	Tool/version, permission decision и status	Чувствительные аргументы по redaction schema
Sharing	Grant/revoke, объект, аудитория и роль	Содержание документа
Infra	Playbook/version, targets, approvals и status	SSH credentials и произвольные команды

Audit защищается от изменения обычными пользователями и сервисами неаудиторского назначения. Отдельные события передаются в SIEM, если это требуется организацией. Trace ID связывает расследование без необходимости копировать весь документ в журнал.

12. Supply chain, обновления и конфигурация

Offline bundle включает images по digest, пакеты, lockfiles, parser assets, Ansible collections, SBOM, checksums, release manifest и known issues. Connected build/import — отдельная контролируемая зона. Контур исполнения не выполняет curl-install или скачивание зависимостей при старте.

Этап	Требование evidence
Сборка	Версия исходников, зависимости, происхождение и воспроизводимый процесс
Проверка	Анализ кода/зависимостей и container images; findings и решение по ним
Импорт	Кто передал комплект, checksum/signature и реестр разрешённых файлов
Установка	Inventory, preflight, migration log и smoke/network checks
Обновление	Backup, compatibility, approved change и health results
Rollback	Что можно откатить и как восстановить данные после несовместимой миграции

Базовые playbooks не выполняют произвольный пользовательский shell. Deployment runner получает только утверждённый playbook, версию и проверенные параметры. Портал не хранит root-доступ ко всем VM как обычный connector.

Global config revisions имеют владельца, diff, область, тест валидации и время применения. Изменение egress, data class, auth или sandbox profile относится к security-relevant change. Runtime/workflow версии закрепляются для активного задания.

13. Backup, устойчивость и инциденты

Backup охватывает metadata/ledger, файловые данные, конфигурацию и необходимый key material по раздельному защищённому процессу. Restore испытывается на чистой инфраструктуре. Replication не заменяет backup от удаления и компрометации.

Событие	Первые действия	Проверка восстановления
Утечка API-ключа	Отключить connector, отозвать секрет, сохранить audit	Новый ключ работает; старый не работает; область ущерба оценена
Подозрение на sandbox escape	Изолировать host/pool, остановить новые runs	Среды пересозданы из проверенного образа; нет persistence
Несанкционированный share	Отозвать grants/links, ограничить affected principal	Cache/export/derived artifacts проверены
Подозрительный egress	Закрыть путь, сохранить gateway/network events	Разрешённая матрица и payload scope восстановлены
Ledger inconsistency	Запретить новые платные операции affected scope	Reservations и проводки сверены
Потеря data service	Включить approved failover/restore	Целостность, ACL, ledger и неоднозначные внешние эффекты проверены

Назначаются incident owner, техническая роль и канал уведомления ИБ. Регламент содержит классификацию, containment, evidence preservation, recovery и review. Уведомления внешним сторонам определяются корпоративными требованиями, не автоматически из модели.

RPO/RTO и доступность согласуются по классу системы. Предлагаемые ориентиры приложения — backup RPO до 15 минут и RTO до двух часов; они требуют измерения. Восстановление не запускает повторную массовую отправку или иной уже выполненный side effect.

14. Реестр угроз и остаточных рисков

ID	Угроза	Основной контроль	Что требует подтверждения
T01	Межпользовательская утечка	ACL всех объектов, cache scope и retrieval controls	Negative tests API/export/SSE/RAG
T02	Prompt injection	Server permissions, отделение данных и tools	Adversarial corpus и trace review
T03	SSRF / DNS rebinding	Network deny, actual-IP/redirect checks	IPv4/IPv6/rebinding tests
T04	Sandbox escape	Изоляция runtime и отсутствие privileged mounts	OS/runtime review и penetration test
T05	Неконтролируемый model egress	Connection policy и data class	Firewall evidence и fallback tests
T06	Secret disclosure	Secret store, minimal exposure и redaction	Scan logs/errors/export/fixtures
T07	Обход бюджета	Atomic reservations и idempotent ledger	Race tests и incomplete-usage fault
T08	Повтор внешнего эффекта	Lease/fencing, outbox и retry classification	Worker partition/replay/restore tests
T09	Вредоносное обновление	Provenance, digests, SBOM и change gate	Release/import evidence
T10	Злоупотребление полномочиями	Separation of duties и audit	Privileged role review
T11	DoS / resource exhaustion	Admission, CPU/RAM/disk/PID limits	Load и malicious resource fixtures
T12	Privacy аналитики	Aggregate ACL, minimization и retention	Review полей, drill-down/export tests

До испытаний остаточный риск не объявляется низким. Для каждого finding фиксируются вероятность/влияние по принятой шкале организации, мера, владелец, срок, результат проверки и решение о допуске. Принятие риска выполняет уполномоченная роль, а не сам агент.

Внешний API остаётся внешней зависимостью: нельзя технически гарантировать правила обработки данных провайдером только настройкой firewall. Эти условия должны быть проверены владельцем подключения и ИБ.

15. Программа security-проверок

ID	Испытание	Ожидаемый результат
STEST01	Подмена user/workspace/object ID	Нет чужих объектов и содержимого в ответах/ошибках
STEST02	Revoke LDAP/local grant	Новые операции закрыты в согласованный срок
STEST03	Просроченный token/share link	Запрет без fallback к более слабому доступу
STEST04	RAG по закрытым chunks	Нет чужого материала в prompt/citations/cache
STEST05	Search private IP/redirect/rebinding	Соединение заблокировано на реальном destination
STEST06	Прямой internet/proxy из sandbox	Запрет всех неразрешённых путей
STEST07	Host socket/secret/mount access	Отсутствие доступа; событие отмечено
STEST08	Oversized/malformed/parser input	Локальный отказ без потери пула
STEST09	Budget race/unknown usage	Нет двойного освобождения и скрытого перерасхода
STEST10	Worker fault/partition	Нет конкурентного внешнего эффекта
STEST11	SMTP changed recipients/retry	Approval invalidated; ambiguous delivery обработана
STEST12	Plugin update/disable	Контракт и permission не обходятся
STEST13	Telemetry/export secret scan	Нет credentials и лишнего содержимого
STEST14	Offline install/upgrade	Нет незаявленных internet-downloads
STEST15	Restore	ACL/ledger сохранены; side effects не повторены
STEST16	Analytics privacy	Недоступные identities/doc names не раскрываются
STEST17	Admin infrastructure action	Только утверждённый playbook/targets; actor и result в audit

Для каждого теста сохраняются версии, условия, входные данные, ожидаемый/фактический результат, ограничения и ссылки на evidence. Penetration test проводится по согласованной области; destructive-тесты — в выделенной среде. Наличие unit tests не заменяет проверку фактической сети и runtime.

Внешние модельные расходы на испытание заранее ограничиваются тестовым бюджетом. Fixtures используют синтетические либо разрешённые данные. Реальные credentials не включаются в исходники и тестовые артефакты.

16. Перечень документов и форма допуска

Документ / evidence	Владелец	До пилота / production
Архитектура и границы системы	Technical lead	До пилота; актуализация production
Классы данных и разрешения внешней передачи	Владелец данных + ИБ	До пилота
Identity/role/access matrix	IAM + platform admin	До пилота
Network matrix и firewall evidence	Сеть + DevOps	До пилота и при изменении
Модель угроз и risks register	ИБ + technical lead	До пилота; закрытие production
Secret handling / rotation	Владелец secret service	До пилота
Sandbox/connector review	Runtime + ИБ	До включения функции
Audit/SIEM и retention	ИБ + оператор	До production
Release/SBOM/update/rollback	DevOps	Каждый релиз
Backup/restore и incident runbooks	Оператор	До production
Security test report	QA + ИБ	Пилот и production
Остаточные риски и эксплуатационные ограничения	Product owner + ИБ	До production

Форма решения

Название и версия приложения; deployment profile; список разрешённых endpoints; категории данных; аудитория и срок пилота; принятые функциональные требования; findings и residual risks; исключения и deadlines; владельцы эксплуатации; перечень evidence; решение «допустить / допустить с ограничениями / не допустить»; согласующие лица и дата.

Данный документ содержит структуру формы, но не подписи и не выполненное согласование. Требования и решения должны быть внесены уполномоченными представителями организации.

Первичные технические источники

- [Keycloak: LDAP и администрирование.](#)
- [MCP: безопасность интеграций.](#)
- [Deep Agents: ограничения локальных backend.](#)
- [Temporal: выполнение и повторы Activities.](#)
- [Docker Compose: production deployment.](#)
- [Anthropic: разделение session, harness и sandbox.](#)

Проверено 02.10.2026. Корпоративные и нормативные требования к системе определяются отдельно организацией.